

## UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of )

(Briefly describe the property to be searched )  
(or identify the person by name and address) )the property at 710 W Historic Mitchell St Apt 220 )  
Milwaukee, WI known and Kunzelmann-Esser Loft )  
Apartments, more fully described in attachment a. )

Case No. 21-942M(NJ)

## WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Eastern District of Wisconsin  
(identify the person or describe the property to be searched and give its location):

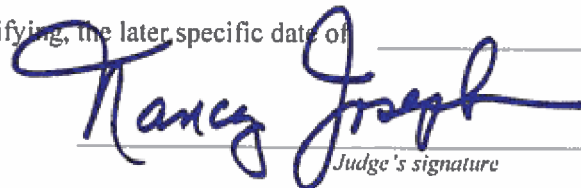
See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B.

**YOU ARE COMMANDED** to execute this warrant on or before July 13, 2021 (not to exceed 14 days)☐ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to \_\_\_\_\_  
(United States Magistrate Judge)☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)☐ for \_\_\_\_\_ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of \_\_\_\_\_.Date and time issued: June 29, 2021City and state: Milwaukee, WI

Judge's signature

Hon. Nancy Joseph, U.S. Magistrate Judge

Printed name and title

**Return**

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: \_\_\_\_\_

\_\_\_\_\_  
*Executing officer's signature*\_\_\_\_\_  
*Printed name and title*

## ATTACHMENT A

### *Property to be searched*

The property to be searched is 710 W Historic Mitchell St Apt 220 Milwaukee, Wisconsin, further described as an apartment complex known as Kunzelmann-Esser Loft Apartments. The exterior of the building appears to be brick, red in color with several windows, an awning red in color and approximately seven stories in height.



## **ATTACHMENT B**

### *Property to be seized*

1. All records relating to violations of wire fraud, bank fraud and money laundering, those violations involving Sona the Voice and occurring after 11/2017, including:
  - a. Records and information relating to a conspiracy to defraud Sharon Metcalfe, Martha Torres, Candy Riggins, Jeffrey and Nesrin Avina, Karen Parness, Madison Smith, Catherine Leggitt, Rocio Gomez De Garcia, Enrique Quintero and Edward Goodwin, and other victims now unknown.
  - b. Records and information relating to the email account sonathevoice@icloud.com
  - c. Records and information relating to the identity or location of the suspects;
  - d. Records and information relating to Ivy League Empire, LCC and Cameroonremit, LLC.
2. Computers or storage media used as a means to commit the violations described above.
3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains, or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
  - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs,

registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;

- b. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- c. evidence indicating the computer user’s state of mind as it relates to the crime under investigation;
- d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- f. evidence of the times the COMPUTER was used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- i. records of or information about Internet Protocol addresses used by the COMPUTER;

- j. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- k. contextual information necessary to understand the evidence described in this attachment.

# UNITED STATES DISTRICT COURT

for the  
Eastern District of Wisconsin

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

the property at 710 W Historic Mitchell St Apt 220  
Milwaukee, WI known and Kunzelmann-Esser Loft  
Apartments, more fully described in attachment a.

Case No. 21-942M(NJ)

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the Eastern District of Wisconsin, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):


- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. Sections 1344, 1343, 1956, & 2	Bank Fraud, Wire Fraud, Money Laundering, Aiding and Abetting

The application is based on these facts:  
See attached affidavit

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

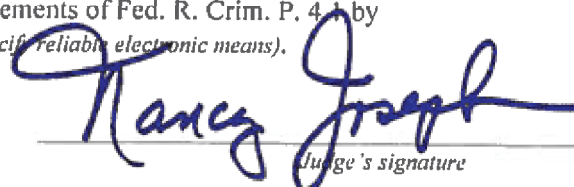
Antonio Murray, USSS Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by  
\_\_\_\_\_ telephone \_\_\_\_\_ (specify reliable electronic means).

Date: June 29, 2021

City and state: Milwaukee, WI



Judge's signature

Hon. Nancy Joseph, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A  
WARRANT TO SEARCH AND SEIZE AND FOR CRIMINAL COMPLAINTS**

I, Antonio Murray, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 710 W Historic Mitchell Street Apartment 220 Milwaukee, Wisconsin hereinafter “PREMISES,” further described in Attachment A, and electronic data on computers and cell phones, herein “RECORDS” for the things described in Attachment B. I also make this affidavit in support of the issuance of criminal complaints against three persons, to be discussed herein.

2. I am a Special Agent with the United States Secret Service and have been so employed since 2019. I am currently assigned to the United States Secret Service Milwaukee Financial Crimes Task Force (MFCTF). My duties as an investigator on the MFCTF include investigations into financial crimes, such as identity theft, check fraud, credit card fraud, bank fraud, wire fraud, currency-counterfeiting offenses, and money laundering. During my time on the MFCTF, I have been involved in investigations that have resulted in seizures of criminally derived property, including monetary instruments.

3. As a Secret Service Agent, I have conducted investigations into wire fraud, money laundering, and other complex financial crimes. In the course of those investigations, I have used various investigative techniques, including undercover operations, reviewing physical and electronic evidence, and obtaining and reviewing financial records. In the course of these



investigations, I have also become familiar with techniques that criminals use to conceal the nature, source, location, and ownership of proceeds of crime and to avoid detection by law enforcement of their underlying acts and money laundering activities.

4. Because I am submitting this affidavit for the limited purpose of establishing probable cause for the requested search and seizure warrant and criminal complaints, I have not included in this affidavit every detail I know about this investigation. Rather, I have included only the information necessary to establish probable cause for the requested search and seizure warrant and criminal complaints.

5. The facts set forth in this affidavit are based on my personal knowledge, including what I have learned through my training and experience as a law enforcement officer, my review of documents and other records obtained in the course of this investigation, my review of other police reports, information provided from law enforcement officers, and information I have obtained in the course of this investigation from the victims of these offenses, all of whom and which I believe to be reliable.

6. This affidavit is intended to show only that there is sufficient probable cause for the requested search warrant and criminal complaints, and does not set forth all of my knowledge about this matter.

### **FRAUD SCHEME**

7. It is believed that suspect Sona The Voice is receiving money from an ongoing “puppy fraud” scheme based in the Milwaukee, Wisconsin area involving online fraudulent advertisements for puppies for sale. The scheme involves in part persons opening bank accounts to receive scheme funds from victims. Victims responding to the online advertisements are instructed to send funds for the purported purchase of a puppy via Zelle, an online payment processing application, to a particular bank account, but victims do not receive a puppy, or anything else. Persons working in behalf of the scheme, known as “mules,” take the Zelle funds from these bank accounts, convert them to cash, and provide the cash to Sona The Voice, who converts the cash into cryptocurrencies, such as Bitcoin. Such cryptocurrencies are largely unregulated, and thus difficult to trace. A cryptocurrency is a digital currency in which transactions are verified and records maintained by a decentralized system using cryptography, rather than by a centralized authority. Cryptography is a technique to send secure messages between two or more participants; the sender encrypts/hides a message using a type of key and algorithm, and then sends this encrypted message to the receiver, who then decrypts it to generate the original message.

8. Evidence gathered so far during the investigation shows that Blair Hudson, Sona The Voice, and Spora Sona were co-conspirators in the scheme, which appears to violate federal laws concerning bank fraud, wire fraud, and money laundering. The federal bank fraud is found at 18 U.S.C. § 1344, and provides, in pertinent part: “Whoever knowingly executes ... a scheme or artifice -- ... (2) to obtain any of the moneys, funds, credits, assets, securities, or other

property owned by, or under the custody or control of, a financial institution, by means of false or fraudulent pretenses, representations, or promises ... [commits an offense]. The federal wire fraud is found at 18 U.S.C. § 1343, and provides, in pertinent part, “Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire ... communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, ... [commits an offense]. The applicable federal money laundering statute is found at 18 U.S.C. § 1956(a)(1)(A) and (B) and provides, in pertinent part, “Whoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts ... such a financial transaction which in fact involves the proceeds of specified unlawful activity – (A)(i) with the intent to promote the carrying on of specified unlawful activity; or ... (B) knowing that the transaction is designed, in whole or in part – (i) to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity [commits an offense]. “Specified unlawful activity” as defined in 18 U.S.C. § 1956(c)(7) and 18 U.S.C. § 1961(1) includes bank fraud and wire fraud. The federal aiding and abetting statute is found at 18 U.S.C. § 2, and provides, in pertinent part, “Whoever commits an offense against the United States or aids, abets, counsels, commands, induces or procures its commission, is punishable as a principal.”

### **PROBABLE CAUSE**

9. On March 23, 2021, your affiant was contacted by Milwaukee Financial Crimes Task Force Officer Detective Lukas Hallmark of the Waukesha City Police Department, who sent me police reports, regarding a motor vehicle stop and interview of one Blair Hudson.

10. On Thursday, March 18, 2021, at approximately 2210 hours, two Waukesha Police officers conducted a traffic stop at Hinman Ave. and Jackson Ct. in Waukesha. During the traffic stop investigation, police arrested Hudson for Bail Jumping, Operating after Suspension, Carrying a Concealed Weapon, Possession of THC, and having an Open Warrant through the Waukesha County Sheriff's Department, and transported to the Waukesha County Jail.

11. During the traffic stop investigation, officers searched the backseat of Hudson's car, and recovered a black fanny pack that contained a large amount of cash bundled with black rubber bands. This packaging is commonly referred to as "stacks", which were bundled in specific amounts: three stacks of \$1 denominations; seven stacks of \$20 denominations; and one stack of \$100 denominations. Waukesha Police later determined that the cash totaled \$18,655.

12. Hudson told police that he had been unemployed since January 2021, and that he hoped to start his own delivery business and contract with Amazon.

13. Hudson told police that the cash was to buy two 2009 GMC cargo vans to start his business, and that he did not keep his money in a bank.

14. During the investigation at the location of the traffic stop, D.W. (02-15-19xx) approached police and said she is the mother of Hudson's child and that Hudson was attempting to visit her before the traffic stop.

15. Hudson told police that he keeps his money with D.W., as he "trusts her". Hudson does not reside with her, but instead another girlfriend in Milwaukee on N. 86th Street.

16. Officers arrested Hudson and searched his person and car, locating three Chase debit cards in Hudson's wallet, which Hudson had on his person. The three debit cards had the following numbers and names:

17. a. J.B. – 4867-9612-1869-98xx

18. b. T.C. – 4427-5612-1034-32xx

19. c. D.H. – 4867-9612-1863-59xx

20. Detective Hallmark interviewed Hudson at the Waukesha Police Department on the morning of Friday, March 19, 2021.

21. A Chase Bank Investigator stated that J.B.'s account was opened in February 2021, however, there was no activity on the account and Chase Bank closed the account in

March 2021. Det. Hallmark learned that D.H.'s account was opened on 2/19/2021 and closed by Chase Bank on 3/12/2021 due to potential fraud. Det. Hallmark learned that T.C.'s account was opened on 2/23/2021 and was closed by Chase Bank on 3/12/2021 due to potential fraud. Chase Bank believed that the accounts were related to a fraud scheme.

22. Later on Friday, March 19, 2021, Det. Hallmark interviewed Hudson for a second time at the Waukesha Police Department after Hudson waived his Miranda rights.

23. Hudson told Det. Hallmark that he recruited individuals from Milwaukee to open Chase Bank accounts online. Hudson further told Det. Hallmark that he would coordinate with an individual named Scott, whom he thought lived in Africa. Hudson would provide Zelle (the aforementioned digital payment network – often used on cell phones) accounts to Scott from the newly-opened bank accounts. Hudson further told Det. Hallmark that money would come into the Zelle accounts that was given to Scott, and when the bank accounts reached approximately \$1000, Hudson withdrew the money, convert it into cash at an ATM, and send the money to the individual in Africa.

24. Hudson told Det. Hallmark that he receives a percentage of the money he sends to Africa, and that the three debit cards he had belonging to T.C., J.B., and D.H. were related to this scheme.

25. Hudson gave Det. Hallmark written consent and passwords and passcodes to search his iPhone and his HP laptop computer, and on March 22, 2021, the Waukesha Police

Department forensically scanned the phone and computer, generating a Magnet Axion Examine report of the iPhone scan. There were no items of evidentiary value on the computer, which was returned to Hudson.

26. The iPhone report contained detailed text conversations. Some “WhatsApp” conversations were between “scott” with a telephone number 2-377-110-1272, and the other person was labeled as “local user”, which indicated that this person was Hudson.

27. The report showed WhatsApp conversations in the iPhone between Scott and Hudson dated from 11/21/2020 at 08:42:39 PM to 3/19/2021 at 1:53:01 AM – a total of 7,223 such messages between Scott and Hudson in that time frame.

28. These conversations almost exclusively concerned exchanges of Zelle, bank and BitCoin account information. Specifically, Hudson would give Scott Zelle and bank account information, and send money to Scott either via Bitcoin, or by giving cash to Scott’s associates in Milwaukee, Wisconsin, who were named Sona The Voice and Spora Sona.

29. The report had a WhatsApp message between Scott and Hudson on November 29, 2020 at 8:57:01 PM, wherein Hudson messaged the following information to Scott:

30. Email: Jsnsusbank@gmail.com, Number: 262-336-0921, Name: J.C.

31. Det. Hallmark knows, based on the context of the conversation and his training and experience, that the information Hudson provided to Scott was for a Zelle account.

32. In another WhatsApp message between Scott and Hudson on December 1, 2020 at 6:37:18 PM, Scott sent Hudson a screen shot of Zelle transfers. The screenshot was of Zelle payments coming into the account of \$250.00 from one K.P. on 11/30/2020.

33. Det. Hallmark found that K.P. was a victim of an online puppy fraud scheme. Det. Hallmark contacted K.P. by phone on April 29, 2021 and learned that she resides in Nevada, and did so at the time of this incident. K.P. indicated she searched the internet to purchase a Havanese puppy, and went to the website [Cassyhavanesebreeders.com](http://Cassyhavanesebreeders.com) and began the purchase process. K.P. indicated she received email correspondence from [Cassyhavanesebreeders@gmail.com](mailto:Cassyhavanesebreeders@gmail.com), which requested payment for the puppy via Zelle. Emails requested that K.P. send a Zelle payment of \$750.00 to an account linked to email address [jsnusbank@gmail.com](mailto:jsnusbank@gmail.com) with name J.C. K.P. indicated her bank only allowed a maximum payment of \$500 per day on Zelle, and that on 11/30/2020, she sent \$500.00 via Zelle to [jsnusbank@gmail.com](mailto:jsnusbank@gmail.com), sent \$250.00 to [jsnusbank@gmail.com](mailto:jsnusbank@gmail.com) the next day from an account linked to her Wells Fargo Bank account and her email address. After she sent the payment, she received a request for \$1500.00 for a crate rental to ship the puppy, which she did not purchase, and stopped communication with [casseyhavanesebreeders.com](http://casseyhavanesebreeders.com). K.P. received neither a puppy nor a refund. Other scheme victims are listed in Attachment B to this affidavit.

34. The report showed a WhatsApp message between Scott and Hudson on 11/30/2020 at 12:02:57 PM, in which Scott said, “then send it to my own cashapp”. Scott later



stated, "Let me send you a video" and " Am talking to Sonna already". Hudson responded, "Ok I'm speaking to Spore now". At 12:06:09 PM Hudson sent Scott a screen shot of a text message with telephone number 414-429-9178. The message read:

35. Hudson: Hey Spora I have some money to give you today to send to Soma

Hudson: Sona

Hudson: Are you available

414-429-9178: Yes Sir

414-429-9178: What time?

Hudson: 10 am

414-429-9178: Bet

36. Det. Hallmark searched Hudson's iPhone for messages with telephone number 414-429-9178 and located 163 SMS/MMS messages sent through iOS messenger (text message) between that number and Hudson in the period between 11/22/2020 at 6:29:24 PM and 3/01/2021 at 10:11:33 PM.

37. Det. Hallmark observed on 11/30/2020 at 12:05:29 PM, Hudson sent a message to 414-429-9178 stating, "Hey Spora I will be dropping money off to you Today ok. I'll be there by 10:30". Telephone number 414-429-9178 stated to Hudson on 11/30/2020 at 1:32:38 PM, "U

just gave me \$9830”. Further messages were then exchanged about Hudson placing money in Bitcoin.

38. The report contained a message between 414-429-9178 and Hudson on 12/30/2020 at 7:21:26 PM. Hudson stated, “Hey I’m down stairs”. On 12/31/2020 at 6:25:07 PM 414-429-9178 stated, “can u pls text me the names and their amounts”. Hudson responded at 7:02 PM stating, “Scott and Clesh”, “Scott 3000”, and “Clesh 640”.

39. Several other text messages in the report indicated that Hudson dropped money off to 414-429-9178 for Scott and Clesh several more times.

40. Det. Hallmark found that law enforcement data bases for 414-429-9178 showed that found that this number was associated with Spora Lyengu Sona, 12/12/1985. Det. Hallmark searched Wisconsin Department of Transportation records which that showed that Sona resides at 710 W Historic Mitchell St, Apt 220, Milwaukee, Wisconsin.

41. Det. Hallmark knows that individuals using Bitcoin often use Coinbase, a cryptocurrency exchange platform. Such a platform is used to buy and sell Bitcoin, Ethereum, and other cryptocurrencies. Coinbase records show that Sona the Voice, 05/25/1986, resides at 710 W Mitchell St, Apt 220, Milwaukee, Wisconsin. Coinbase records also included a Wisconsin Photo Driver’s license of Sona the Voice along with a webcam photo of Sona the Voice.

42. On March 30, 2021, your affiant obtained a federal seizure warrant for \$18,655 in funds found in Blair Hudson's possession on March 18, 2021, now being held in evidence by the Waukesha Police Department.

43. The State of Wisconsin's Department of Financial Institutions records show two businesses listing Sona The Voice as the registered agent: Cameroonremit, LLC and Ivy League Empire, LLC. Ivy League Empire, LLC lists its principal office at 710 W Historic Mitchell Street, Apartment 220, Milwaukee, WI. Cameroonremit lists its registered agent office at 2266 N Prospect Avenue Suite 316, Milwaukee, WI. Agency records list Sona The Voice as the 100% beneficial owner of both businesses.

44. Coinbase's records provided several photos from Sona The Voice's account. One of the two photos was of Voice's Wisconsin Driver's License, and the other a photo of Voice taken with what appears to be a webcam attached to Voice's computer. Several bank accounts show Fedwire payment information to numerous beneficiaries, including Spora Sona, Sona The Voice, and Ivy League Empire, LLC. Activity in this Coinbase was between 11/30/2017 and 04/06/2021. During this timeframe approximately 80 "wallets" were created. A "wallet" in this context is a device, physical medium, program or a service which stores the public and/or private keys for cryptocurrency transactions. A "public key" for such a transaction allows an individual to receive cryptocurrency transactions. The public key receives transactions in the form of an address, which is a shortened form of an individual's public key. A "private key" for such a

transaction is an individual's ability to prove ownership or spend the funds associated with an individual's public key. It typically takes the form of a 256 character-long binary code, 64 digit hexadecimal code or Mnemonic phrase. In addition to this basic function of storing the keys, a cryptocurrency "wallet" also offers encrypting and/or signing information. Several log-ins were time-stamped during the period this account was active, which occurred in the United States, Cameroon, or Belgium, and showed the following cryptocurrency transactions: 166 Bitcoin, 43 Ethereum, 3 Litecoin, among various other cryptocurrencies. The total amount of USD deposited in this Coinbase account was \$1,733.470. Sona The Voice and Ivy League Empire, LLC were names on the seven bank accounts linked to the Coinbase account which were used to purchase cryptocurrency.

45. Records from J.C.'s Square bank account, which was accessible by Hudson, show the following:

46. During the same timeframe of J.C.'s involvement in the scheme, from November thru December of 2020, six transactions were attempted or completed on this Square bank account, in amounts ranging from \$100 to \$500. In each of the subject's comments on each of the transactions posted on J.C.'s Square account, the following notations were observed: "Puppy \$\$\$," "Joniel (dog deposit)," "Puppy," "puppy deposit," and "🐶🏠🐶🏠" (which is emoji or symbol for a puppy). J.C. also sent and received funds in these transactions.

47. The other name that connects Hudson to Spora and The Voice is an individual known as “Elias”. Multiple times, an individual named “Elias” sent and received funds from Hudson, Spora, or Voice, ranging in amounts from \$100.00 to \$2,000, and occurring from 04/2020 until 01/2021.

48. Text messages in the Waukesha PD forensic report showed that Spora Sona received the funds from Hudson in the fraudulent “puppy fraud scheme”. Records of Square, a financial services and digital payments company, showed that Sona did unlicensed Money Services Business (“MSB”) financial transactions similar to Voice’s activities. A MSB financial transaction transmits or converts money. MSBs must be registered with the Financial Crimes Enforcement Network (“FinCen”) which analyzes financial transactions to combat financial crimes. On 10/13/2020, Sona received \$2,500 from D.D., and within minutes conducted an exchange of currency for \$2,000. Sona’s account showed comments: “money for cameroon,” “cameroob,” “business with the Voice,” “For the Voice Business,” “Business (The Voice),” “For cameroon,” “for voice,” “For the Voice,” and “For Cameroon and payment for sona, business”. The Square account financial activity also shows one sender, D.N., sending and attempting to send Sona’s account an approximate total of \$70,000 between 06/10/2020 and 06/16/2020. Sona listed employment as a Certified Nursing Assistant according to database sources, however, this assertion could not be verified with WI nursing records. During the activity on the Square account, Voice sent Sona numerous transactions, ranging from \$100 to \$4,100.

49. On June 7th, 2021, your affiant spoke with personnel at Educator's Credit Union ("ECU") regarding contacts with Voice, and Voice's activity on Voice's ECU account. ECU contacted the Voice regarding certain unusual account activity on 04/10/2020, who advised he was purchasing large sums of Bitcoin and holding it until the price increased, whereupon he would sell it. Voice advised ECU he did not send the wires to purchase the Bitcoin from his business account because he cannot track funds not coming from an account in his name.

50. After several suspicious transactions, ECU stopped all wire activity on the account, which Voice did not challenge, tending to confirm to ECU that the account was not used for legitimate business purposes.

51. Between March and August of 2020, records for Voice's Square account showed that various individuals either completed or attempted 14 transactions to Voice. In the subject lines of the transactions the following notes were observed; "Hello Send to Cameroon," "for Cameroon," "Enanga Cameroon," "for Cameroon," "Cameroon transfer," "transaction to Cameroon," "to Cameroon," "for Cameroon, thx," "Money Transfer," and "CMR Remit and CR Transactions".

52. Voice listed himself on the Wisconsin Department of Financial Institution's website under a search of corporate records as the owner of Cameroonremit, which advertises itself as on its website Cameroonremit.com as a leading MSB in the United States. Neither of Voice's businesses are registered with FinCen as a MSB.

53. On May 27, 2021, Det. Hallmark and your affiant interviewed J.C., 12/04/20xx, in West Allis, Wisconsin. J.C. said that Hudson had been an associate since November 2020, and solicited J.C. to participate in a puppy sale scam, instructing him to open bank accounts at JP Morgan Chase and US Bank to receive scheme funds. Hudson gave J.C. access to the US Bank and Chase Bank accounts through Zelle accounts. J.C. said that approximately \$10,000 came into the accounts every other day, whereupon he withdrew the money from the account in cash and gave it to Hudson, who then gave it to an individual in another country. J.C. said that Hudson was paid for his participation, and that Hudson paid him a total of \$300.

54. On June 11, 2021, at approximately 12:40 PM, Det. Hallmark and your affiant met with M.C. at West Allis, Wisconsin, who confirmed her identity. M.C. indicated she was with Hudson two or three times when he dropped off “puppy scam money” between about November, 2020 through January 2021 to an individual in Milwaukee, Wisconsin, which he did to make money. M.C. indicated that the recipient of the cash from Hudson was also part of the fraud scheme, and that she was with Hudson when he called this individual and spoke to them on a speaker phone. M.C. didn’t know the exact location but would remember it when she saw it and would identify the building for investigators. She described the building as a multi-level apartment building with retail shops underneath, an awning over the front door, and a parking lot across the street.

55. Also on June 11, 2021, M.C. rode with your affiant and Det. Hallmark in Milwaukee and identified with certainty an apartment building located at 710 W Historic Mitchell St, Milwaukee, Wisconsin, as being the place where she had been with Hudson when he dropped off scam money.

56. M.C. said she would park on South 7th St across from the apartment building, and Hudson would walk into its lobby and meet with a black female of average build with dreadlocks. M.C. saw Hudson give cash to this female, then after one or two minutes leave the lobby and get back into the car, without going upstairs into the apartment. M.C. indicated the cash would usually be in an envelope, such as a bank envelope.

### **TECHNICAL TERMS**

57. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

### **COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

58. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One



form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the proposed warrant would authorize the search and seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

59. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, to include all occupants, any common storage facilities, any buildings or storage building located on the curtilage, any safes or secure storage containers, and any vehicles on the property or curtilage or on the street directly associated with the occupants at the above location for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”
- e. Based on actual inspection of other evidence related to this investigation, spreadsheets, financial records, invoices, I am aware that computer equipment was used to generate, store, and print documents used in the money laundering

scheme. There is reason to believe that there is a computer system currently located on the PREMISES.

60. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the

sequence in which they were created, although this information can later be falsified.

- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpatng or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the

computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect(s). For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
  - d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
  - e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
61. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often

requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and

configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

62. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

63. Because several people may share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is



possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

### **CONCLUSION**

64. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B for evidence of the federal offenses of wire fraud, bank fraud, and money laundering, as well as for the issuance of criminal complaints against Blair Blake Hudson, Spora Lyengu Sona, and Sona The Voice.

### **ATTACHMENT A**

#### *Property to be searched*

The property to be searched is 710 W Historic Mitchell St Apt 220 Milwaukee, Wisconsin, further described as an apartment complex known as Kunzelmann-Esser Loft

Apartments. The exterior of the building appears to be brick, red in color with several windows, an awning red in color and approximately seven stories in height.



## **ATTACHMENT B**

### *Property to be seized*

1. All records relating to violations of wire fraud, bank fraud and money laundering, those violations involving Sona the Voice and occurring after 11/2017, including:
  - a. Records and information relating to a conspiracy to defraud Sharon Metcalfe, Martha Torres, Candy Riggins, Jeffrey and Nesrin Avina, Karen Parness, Madison Smith, Catherine Leggitt, Rocio Gomez De Garcia, Enrique Quintero and Edward Goodwin, and other victims now unknown.
  - b. Records and information relating to the email account sonathevoice@icloud.com
  - c. Records and information relating to the identity or location of the suspects;
  - d. Records and information relating to Ivy League Empire, LCC and Cameroonremit, LLC.
2. Computers or storage media used as a means to commit the violations described above.
3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains, or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
  - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs,

registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;

- b. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- c. evidence indicating the computer user’s state of mind as it relates to the crime under investigation;
- d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- f. evidence of the times the COMPUTER was used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- i. records of or information about Internet Protocol addresses used by the COMPUTER;

- j. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- k. contextual information necessary to understand the evidence described in this attachment.